NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

A CYBERCIEGE SCENARIO TO ILLUSTRATE CLASSIFIED INFORMATION MANAGEMENT IN MULTILEVEL SECURE SYSTEMS FOR MILITARY COMMAND AND CONTROL

by

Ng Chee Mun

December 2005

Thesis Advisor:	Cynthia E. Irvine
Thesis Co-Advisor:	Paul C. Clark
Second Reader:	Michael F. Thompson

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2005	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE: A CyberCIEGE Scenario To Illustrate Classified Information Management in Multilevel Secure Systems For Military Command and Control	**5. FUNDING NUMBERS**
6. AUTHOR(S) Ng Chee Mun	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited	**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

Raising the awareness of information security has been the focus of DOD and other government agencies in recent years. There is a need for an effective means of educating and training personnel in the topic of Information Assurance. CyberCIEGE offers an approach to training by engaging the personnel in an interactive simulation-based network security game. Each game scenario in CyberCIEGE is designed to impart some network security principles and Information Assurance concepts to the players.

This research developed a scenario definition file for the CyberCIEGE game engine to illustrate and train players on matters related to information protection using compartmentalized Mutlilevel Secure (MLS) systems. The specific area of research is on the protection of sensitive information and operational commands for command and control systems. Through playing this military-based scenario, players can learn about the importance of physical security, the different strategies to protect sensitive information, and the use of MLS systems to provide controlled access to sensitive information. Testing of this game scenario was conducted through the creation of detailed solutions and incorrect gameplay examples.

14. SUBJECT TERMS Multilevel Security, Computer Game, Training, Information Assurance, CyberCIEGE, Computer Security	**15. NUMBER OF PAGES** 80
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

A CYBERCIEGE SCENARIO TO ILLUSTRATE CLASSIFIED INFORMATION MANAGEMENT IN MULTILEVEL SECURE SYSTEMS FOR MILITARY COMMAND AND CONTROL

Chee Mun Ng
Civilian, Ministry of Defense, Singapore
B.S., (Hons), National University of Singapore, 1996
M.S., National University of Singapore, 1999

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
December 2005

Author: Chee Mun Ng

Approved by: Cynthia E. Irvine
Thesis Advisor

Paul C. Clark
Thesis Co-Advisor

Michael F. Thompson
Second Reader

Peter J. Denning
Chairman, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Raising the awareness of information security has been the focus of DOD and other government agencies in recent years. There is a need for an effective means of educating and training personnel in the topic of Information Assurance. CyberCIEGE offers an approach to training by engaging the personnel in an interactive simulation-based network security game. Each game scenario in CyberCIEGE is designed to impart some network security principles and Information Assurance concepts to the players.

This research developed a scenario definition file for the CyberCIEGE game engine to illustrate and train players on matters related to information protection using compartmentalized Mutlilevel Secure (MLS) systems. The specific area of research is on the protection of sensitive information and operational commands for command and control systems. Through playing this military-based scenario, players can learn about the importance of physical security, the different strategies to protect sensitive information, and the use of MLS systems to provide controlled access to sensitive information. Testing of this game scenario was conducted through the creation of detailed solutions and incorrect gameplay examples.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to express thanks to many individual who have influenced and assisted me during the development of this thesis.

I would like to express thanks to Prof. Cynthia Irvine, Paul Clark, and Mike Thompson, my advisory team. Thank you for your patience and constructive comments, especially when I struggled to express the concepts involved with this thesis.

I would also like to thank Mary Mulligan for the excellent and professional support for improving my American English writing style.

Finally, I also wish to thank my sponsor, the Defence Science and Technology Agency (DSTA) for the scholarship to participate in this enriching experience at the Naval Postgraduate School in Monterey.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. THESIS STATEMENT

This thesis research is part of the ongoing research project called CyberCIEGE, conducted at the Naval Postgraduate School. The purpose of CyberCIEGE is to develop a computer-based game to teach network security and Information Assurance concepts to military personnel and to students in introductory computer security courses.

The question that this thesis answered was: is it possible to develop a CyberCIEGE Scenario Definition File (SDF) that can illustrate the principles of Multilevel Security (MLS) systems and how they can be deployed to protect different classes of sensitive information and their application in a military context?

B. THESIS SCOPE AND LAYOUT

The scope of this thesis research is to develop a scenario definition file for the CyberCIEGE game engine to illustrate and train DOD personnel and students in the introductory computer security courses on matters related to information protection using Multilevel Security (MLS) systems. Research was focused on the protection of sensitive information in a Command and Control (C2) center, primarily on the protection of different classes of information in storage and transmission. This information forms part of the virtual characters' assets, e.g. command information, structure information, databases etc. Failure to protect such information might result in the compromise of state secrets and the failure to accomplish military missions.

A test plan was developed to test whether the scenario behaves as might be expected in a real-world scenario. The impact of this research could benefit future DOD training and education requirements in the Information Assurance or Computer System Security areas, as well as educational benefits in the civilian sector.

This thesis is comprised of the following chapters:

- Chapter I – Introduction. This chapter provides the thesis statement and defines the scope for this thesis. It gives an overview of the chapters and annexes to this work.

- Chapter II – Background. This chapter describes the CyberCIEGE project, provides the background to the issues for this thesis and illustrates the contribution of this thesis to the overall CyberCIEGE project. It describes the need for the management of classified information, what a multilevel system is, the need for high assurance, and how high assurance multilevel components can be used to provide controlled sharing of classified information.

- Chapter III – Scenario Goals. This chapter spells out the three educational goals that are to be achieved through the design of this scenario. It also identifies the intended players who will benefit from playing this scenario.

- Chapter IV- Scenario Description. This chapter describes the simulated gaming environment modeled by the SDF. It includes the scenario's narrative, briefing to the player, a description of the users in the game and the assets that the players must protect.

- Chapter V – Testing. This chapter describes the test strategy and test cases that were designed to verify the scenario. It includes the scope, expected and actual results of the testing conducted.

- Chapter VI – Conclusion. This chapter summarizes the work accomplished for this thesis and proposals for future research.

II. BACKGROUND

This chapter provides a description of CyberCIEGE and issues concerning the management of a multilevel secure system. Readers are encouraged to read [IRVINE 2003] and [SMITH 2005] for more in-depth discussions of these topics.

A. GAMING, THE NEXT GENERATION OF TRAINING IN THE INFORMATION AGE

In our phase of the information age, the computer has literally penetrated all forms of deployment from number crunching office processing to real-time air traffic control systems, as well as mission-critical military applications (such as Command and Control systems). The fast processing and accurate computing capabilities of the computer have rendered numerous functional and economical advantages. Today the computer has become one of the indispensable and common assets that any organization needs.

According to [PRENSKY 2003], the proliferation of personal computers and the introduction of digital games have changed the way we learn and interact with computers. Computer games have become the alternative tool for cost effective training of a game savvy generation of soldiers; soldiers learn by playing the different scenarios of the game, and pitting the skills they acquire in the classroom lectures against the computer game engine in order to complete and win. Many institutions all around the world are using gaming tools to educate and motivate their students to learn and acquire new skills. As cited in [Fong 4004] and [Zyda 2003], military organizations are also beginning to deploy and make use of COTS gaming for their ongoing training and military experiments. The advantages of leveraging computers are multi-fold. First, it is low risk as it does not involve deploying actual equipment like weapons or exposing systems to adversarial attacks. Without such deployment, the gaming is also more economical. Second, it taps the experience of senior officers to create scenarios which depict real occurrences in relatively short development time. Last, incorporation of computer gaming into training curriculum saves training resources and increases realism through the conduct of distributed gaming involving multiple parties. With these advantages, gaming is rapidly becoming an integral part of the educational toolset.

B. CYBERCIEGE

One objective of the Center for Information Systems Studies and Research (CISR) at the Naval Postgraduate School is to provide improved information assurance education and training for the U.S. military and government. The CyberCIEGE program was initiated by CISR as one strategy to achieve this objective: to develop a gaming tool to convey knowledge about Information Assurance (IA) and at the same time teach users to apply this knowledge and skill in a variety of situations [IRVINE 2003]. The goal of CyberCIEGE is to provide a simulated virtual deployment environment where players internalize concepts by playing CyberCIEGE. Through CyberCiege, players learn and understand how computer architectures and infrastructures can be compromised or protected. In doing so, it is hoped that CyberCIEGE will impart knowledge about the general concepts of computer and network security, and the measures that could be taken to improve the protection of sensitive and critical information.

CyberCIEGE is a security simulation game that simulates a range of scenarios to engage the users in applying their computer and network security concepts to complete these games. Each scenario depicts an organization with some pre-defined users and assets. The users work and earn money for the organization. In order to be productive, these users have to access assets as part of achieving their goals. Assets are information that is valuable to the organization for example: weapon specifications, military operations strategies, and organizational development plans. As such, these assets are also of interest to the competitors and adversaries who may use this knowledge against the organization. Competitors will resort to all means to capture these assets.

The objective of each scenario will be for the players to make money for the organization by keeping the users happy, allowing them to achieve their goals by accessing assets, and avoiding penalties when the security policy is violated, which will compromise the assets. Players of CyberCIEGE have to provide the necessary resources and environment needed by the users to reach their goals. The players will purchase and set up computers and network equipment to facilitate the users' access to their assets. By connecting the computer systems, these assets become available via the network which the users can access. However, there is risk involved when connecting the assets to the network; competitors and adversaries will exploit these network connections to capture the assets. Therefore, a tension exists between risk mitigation against security policy violation and the requirement to allow users to accomplish their tasks.

The player assumes the role of the defender of some important assets in each scenario; his tasks will include setting up and configuring the computer and network infrastructures to achieve the designated operational goals. He will make security-relevant decisions about the systems to deploy, the network components and their interconnections. The simulator, on the other hand, will respond by generating attackers who may exploit any vulnerabilities or gaps in the infrastructure to compromise the valuable assets and undermine the security of the network. The simulator can assume many adversarial roles, such as incompetent users, vandals, and professional attackers, to simulate various types of attacks. To ensure security, the player must install sufficient security measures to allow the virtual characters in the games to achieve their operational goals without compromising the security.

Ultimately, CISR envisages that CyberCIEGE will become an integral part of the educational tools for all information assurance training in the U.S. military and government. The advantages of using CyberCIEGE are as follows: first, it exposes players to various practical scenarios so that they can learn by virtual implementation of the required computer infrastructure. The experiences gained through going through these scenarios will be valuable to the players as they can apply what they have learned to their actual ground deployment. The scenarios are configurable to depict actual deployments, and players can run them repeatedly to try out various alternative implementations to evaluate their strengths and weaknesses. Hence it is much cheaper and less risky to run computer simulations than to provide actual test beds for gaining such experiences. Eventually CyberCIEGE will complement conventional classroom and seminar-style teaching to provide a more interactive and engaging learning environment.

C. MANAGEMENT OF CLASSIFIED INFORMATION

Government departments and private organizations need to protect their sensitive information. For a business organization, sensitive information includes operational processes which provide the company's competitive advantage and hence its survivability, or trade secrets from which the company gains its profit. For a government to ensure the nation's survival, it must religiously control sensitive information that may give the nation a significant advantage over its adversaries and prevent enemies from gaining advantages that could potentially damage the nation. Such information is jealously protected and not shared with unauthorized persons.

The defense community, in particular, because of the nature of its work to protect the nation's sovereignty, will always protect national secrets and sensitive information. Such information includes the country's military operations, intelligence information gathered about adversaries, discussion about diplomatic activities and issues concerning national security and national affairs. The military also possesses information and technologies which could be helpful to the enemy, and if such information is released without authorization, it will compromise the nation's security. Such compromise can result in battles lost, operations compromised, and death and injury to military personnel. There is a need to protect and control this information.

The military protects information through the use of a classification system. Sensitive information is partitioned into a set of equivalence classes which have associated labels. Access is based upon label comparison. This provides protection and controlled access to the information. Sensitive information is normally classified based on the severity and impact of its compromise. In the U.S, there are three levels of classification: TOP SECRET, SECRET and CONFIDENTIAL, in decreasing order of sensitivity. TOP SECRET information is information that if leaked will cause exceptionally grave damage to the nation's security. This includes weapon designs, intelligence and national security information. SECRET and CONFIDENTIAL information must also be protected, but the impact of its disclosure is less severe. SECRET information applies to that information that could cause serious damage to national security when disclosed without authorization. A CONFIDENTIAL classification is applied to information when disclosed without authorization will cause damage to the national security. Information that is not in these sensitivity levels is unclassified.

To access classified information, personnel must have appropriate security clearance and have a need to know the information. Security clearance statuses are assigned for some members of the military community, government departments and contractors to allow them to have access to the classified information. Such clearances are granted through a formal investigation process to assess the member's credentials and character. These processes involve background checks, credit history reviews and agency-specific examinations [FBI 2005]. Depending upon the type of classified information involved, the required security clearance will vary and all clearance status will be renewed periodically. When granted the appropriate security clearance, members can only access classified information on a "need to know" basis.

Classified information is critical to decision making because it provides insights into a situation as well as undisclosed facts that are instrumental to issues to be discussed and detailed information about the domain. Classified information is assimilated and analyzed into reports to enhance the decision makers' judgments on the issues and thus increase the effectiveness of decision making. However, decisions are usually not made based on information from one classification alone. Critical decisions like decisions to launch military operations, merge companies, or decisions to develop or purchase certain weapon systems, are carefully deliberated. Informed decisions are only made when information from various sources is consolidated to provide an overall picture which is then appraised and decided on. Government departments and agencies should not operate as a loosely coupled environment, but as a closely collaborative and integrated unit. Decisions are made over evolving negotiation and decision-making processes. Similarly, in the military, missions and operations are carried out as an integrated force with the support from all services and operational units. The Navy, Marine and Air Force combined their efforts as joint operations in Operation Enduring Freedom [GlobalSecurity 2005], and Operation Iraqi Freedom. As the world becomes more connected, battles and wars against threats to peace, for example, the war against terrorism, will not be fought by an individual nation, but as a joint effort among the countries to maintain peace and order across the globe. Therefore, there is a need for information from different sources with different sensitivity levels to be merged for processing and integration. Officers will need to access information across multiple sensitivity levels in order to achieve their objectives and carry out their jobs. There is a need for a more efficient, interoperable and secure infrastructure to share this information.

D. INFORMATION SECURITY

The secure management of classified information has always been a challenge to the computer security community. For any management of classified information, security policies are needed to define the rules to govern the protection of the sensitive information against potential threats. Based on the security polices and the types of computer components used, different operating environments will be set up. In a dedicated mode of operation where protection is provided by physical means external to the computers, the computers are not equipped with stringent security mechanisms. Examples of such physical means are fences, guards, motion alarm systems, biometric zone access, and so forth. In this mode of operation, all users have clearance and a need to access the highest classified information in the computer systems, and the computer systems are not connected to a network beyond the physical perimeter of the secure zone. Everything within the physical perimeter is considered to be secured. In such situations, security policy is enforced at the physical boundary and not at the computer systems.

In a single level security system environment, the computers are equipped with internal security mechanisms to protect the sensitive information and control the users' access to this information. Not all users are granted access or have the need to access all the information. Based on the users' logins to the systems, the access control mechanism in the computer systems will regulate the information that they can access. Single level security systems protect information of the same security classification; information of different classifications is stored in separate single level security systems. Internal security mechanisms are built into the single level security systems to enforce the access control policy.

As the advancement of technology is exploited to further manage different classifications of information, verified and trusted mechanisms must be put in place within these computer systems to distinguish different levels of information and different levels of user authorizations and access. This gives rise to the multilevel systems, which compartmentalize information of different classifications, and protect and control access to the classified information. These multilevel security systems have internal mechanisms to enforce the security policy and provide some level of assurance that their functionalities and mechanisms do so robustly and reliably. Secure information infrastructures are also needed to protect information of different classifications from users with different security clearances.

In addition to these operational requirements, basic information security pervades all such needs. The basic information security objectives are confidentiality, integrity and availability. To ensure confidentiality, information must be disclosed to authorized persons only. Integrity of information is important to ensure that information is not unintentionally and maliciously modified in storage or in transmission. Equally important is the need for information to be available at all times regardless of attacks or breakdown of services. Three key mechanisms are important to achieve confidentiality, integrity and availability: a) authentication to establish the identity of the entity using the system, b) access control to restrict the access of information to only legitimated users, and c) audit trails to records all activities related to this information.

1. Secure Systems

According to [DOD 5200.28], the features of a secure computer system are as follows:

> Secure systems will control, through use of specific security features, access to information such that only properly authorized individuals, or processes operating on their behalf, will have access to read, write, create, or delete information.

To implement such a system, the following fundamental requirements must be met. First, there must be a security policy that defines a set of rules from the management governing the usage of computer systems for information processing. It determines whether a given subject can be permitted to access a particular object. The security policy’s objective is to serve as:

> A statement of intent with regard to control over access to and dissemination of information, to be known as the security policy must be precisely defined and implemented for each system that is used to process sensitive information. The security policy must accurately reflect the laws, regulations, and general policies from which it is derived [DOD 5200.28].

Using the security policy, rules are implemented in computer systems to enforce the policy. These rules will mandate the life cycle management of classified information, and the access control of this information. Based on the subject’s clearance and authorization to the information, and the classification of the information, these rules will determine the mode of access the subject has to the information. These rules, known as mandatory security controls, are non-discretionary and will apply to all information stored in the computer system and entities that access that information. Mandatory security controls should correctly reflect the security policy. For more granular control of information within mandatory security control, discretionary security controls are introduced. Discretionary controls provide users with the ability to control and limit access of information based on the individual’s discretionary need-to-know requirement for that information.

All objects in the computer system must be classified according to their sensitivity levels. Active entities in the system, subjects, will have modes of access to the objects, that is, read only, write only or a combination of these access modes. The secure system must maintain the integrity of this security classification and the information so that mandatory access controls can accurately mediate access. Similarly, all subjects that access the objects in the system must be identified, and the subject’s access must be mediated by the access control mechanisms. Identification of the subjects is done through the authentication mechanisms which represent to the system the subject’s clearances and need to know for information. Based on a subject’s clearance and need to know, mandatory and discretionary controls are invoked. All activities carried out by the subjects must be reliably maintained in the system.

The computer system must provide an audit trail to trace actions that affect the security of the system. It must reliably record security-related activities in an audit log and protect them from unauthorized amendment and destruction. These audit records may be used for subsequent investigations into system violations, if necessary.

The system must provide mechanisms that enforce the above requirements. The designs of these mechanisms must comply with some mathematical formal methods and they must be properly implemented using rigorous controls and proven standards. The system must ensure that these enforcing mechanisms are themselves being protected against any forms of unauthorized modifications and compromise. In addition, these mechanisms should be evaluated to provide assurance that the system enforces the security policy.

2. Reference Monitor Concept

To describe the enforcement mechanism for authorized access control between the subjects and objects, the reference monitor concept was introduced by James P. Anderson in the 1972 Computer Security Technology Planning Study [Anderson 1972].

> The function of the reference monitor is to validate all references (to programs, data, peripherals, etc.) made by programs in execution against those authorized for the subject (user, etc.). The reference monitor not only is responsible to assure that the reference are authorized to shared resource objects, but also to assure that the reference is the right kind (i.e., read, or read and write, and etc.). [Anderson 1972]

The reference monitor enforces the authorized access relationship between subjects and objects of a system, and this forms the basis for development of systems that provide secure sharing of resources. The implementation of the reference monitor is known as the reference validation mechanism (RVM). It is the hardware and software that implements the reference monitor concept. RVM mediates all references to objects based on the subject’s access rights stored in the system’s access control database. The reference monitor concept and its implementation, that is, RVM, are essential notions of high assurance systems that provide multilevel secure computing facilities and controls.

3. Multilevel Secure System

The interdependence of multilevel classified information and security clearances of users introduces the concept of multilevel security and multilevel security (MLS) systems [Smith 2005]. In the early deployments of systems that process classified information, separate single level computers and networks were used to handle information of different security classifications. This prevents uncontrolled sharing of information across different classifications and prevents leakage of higher classified information to those of lower classification. However such deployments had disadvantages: there was a lot more equipment to manage, different networks to maintain, and users had to physically switch between systems to access information of different classifications. Thus, such solutions were costly, difficult to maintain and troublesome to use. The defense industry began to research ways in which dedicated high systems could be used to access different classifications of information while reducing the cost in deploying multiple systems and networks. Periods processing was introduced. Periods processing established protocols, by which users can connect their computers to networks at one classification, process the information, sanitize the systems and reconnect them to other networks of different classifications. This allowed the same set of systems to be used to access information with different classifications. However, periods processing did not address the need to access information from multiple networks simultaneously and offered little improvement to the separate systems and networks solution.

The concept of a MLS system is a system that can process information of different security levels, label and isolate information at the appropriate levels and share the information only to the appropriate cleared users. In order to achieve such secure sharing of classified information, MLS systems require a set of security mechanisms to ensure that access to this classified information is strictly controlled according to some predefined security policies. These security mechanisms must be reliable, robust, and built with assurance such that they are invoked consistently and cannot be compromised or subverted. Independent third-party testing and evaluation is conducted to review and analyze the implementation to provide an unbiased assurance assessment that the system does enforce the defined policies diligently.

In an MLS system, all entities have security-relevant attributes or labels associated with them. Subjects are active entities that cause information to flow among objects. In computer systems, subjects are processes and applications that run on behalf of the users. Based on the users' access rights and log in sessions, subjects inherit a subset of the users' authorized permissions to access certain objects, the modes of access and the security levels of the login session. Objects, on the other hand, are passive entities that store information. Objects have access control lists and security class labels, which together signify the security classification and access rights to the information that the objects hold. The interaction among these entities often follows the following principles:

- Subjects may share information among themselves if they are of the same sensitivity level.
- Lower sensitivity level subjects can write information to higher security level objects, but they cannot read information from the higher security objects.
- Higher sensitivity level subjects can read information from the lower security objects but they cannot write information to lower security level objects.

These principles enforce the "write down and read up" security restrictions. They allow a user with the security access level of SECRET to retrieve information from the lower security levels, like CONFIDENTIAL, and write up to TOP SECRET information. However, these restrictions will disallow this user to read TOP SECRET information or write CONFIDENTIAL information, in the absence of a trusted mechanism [DOD 5200.28]. Hence, the MLS system must be equipped with an internal mechanism to enforce the security policy.

4. Bell-LaPadula Security Model

In 1974, the Bell-LaPadula security model was introduced. The Bell-LaPadula security model defines a set of restrictions that is essential to providing secure protection of classified information in a multilevel security system [LaPadula 1996]. It enforces MLS access control with the following subset of rules:

a. Simple Security Property (Confidentiality)

A subject can read from an object as long as the subject's sensitivity level is the same as or higher than the object's sensitivity level. This property implements the no read up requirement; that is it prevents subjects from reading information the sensitivity level of which exceeds the subject's sensitivity level.

*b. *- Property (Confidentiality)*

A subject can write to an object as long as the subject's sensitivity level is the same or lower than the object's sensitivity level. This property implements the no write down requirement; that is, subjects with a higher sensitivity level cannot pass information to users or objects of a lower sensitivity level.

The Bell-LaPadula security model is consistent with the MAC secrecy policy for the enforcement of controlled access to classified information. It effectively ensures and protects the confidentiality of the information and prevents the flow of information via "read up" and "write down", as required by an MLS system. As a result, most MLS systems and components implement security mechanisms that enforce the Bell-LaPadula security model.

c. Limitations of Bell-LaPadula Security Model

There are some inherent operational limitations to the Bell-LaPadula model. First, the policy imposed by the MLS access control can hinder operational and security needs. In the design of a Command and Control system, TOP SECRET information is used to determine the course of actions and is then translated into tactical commands for ground troops to execute. Such tactical commands are passed downward in digital form via encrypted voice communication links which have only SECRET security classification. Therefore, there is an operational need to downgrade TOP SECRET information into SECRET information so that it can be transmitted via the SECRET channel to the ground troops on the field. Such downgrading of information has to be done through trusted subjects, or manual sanitization and reclassification by officers before this information is disseminated through the appropriate channels [DOD5200.28].

Second, developers of MLS systems discovered that it is extremely difficult to completely prevent information flow across different security levels. All computer operating systems share resources, like memory and CPU timing, among processes to optimize performance. In sharing these resources, the operating systems may open channels for processes to exchange information. Thus it is difficult to prevent covert channels [Cohen 1990]. Building a system to ensure that the Bell-LaPadula model's flow of information is enforced at all times requires considerable sophisticated security engineering.

Last, the Bell-LaPadula model allows information to flow from low to a high security level; this is consistent with the security policy governing the secrecy of classified information. However, the Bell-LaPadula model does not address the integrity of classified information, that is, it does not prevent some low integrity information or low secrecy classification from writing up to information of a higher classification. This can compromise the integrity of the more highly classified information. For example, if malicious applications are introduced, they can flow to the high security entities, and corrupt and amend the highly classified information without authorization. To some degree, malicious applications like viruses can replicate themselves in the systems they infect. If a virus is implanted at the unclassified level of an MLS system implementing the Bell-LaPadula model, the virus can potentially spread to the higher sensitivity levels of the MLS system. Integrity of classified information is addressed by different polices with a different set of security rules and models, for example, the Biba integrity model.

5. Biba Integrity Model

Another model that is of relevance to the protection of classified information in a MLS system is the Biba security model. While Bell-LaPadula model protects against the flow of sensitive information to less sensitive components in the MLS system, the Biba model protects high integrity information from being modified by low integrity subjects. Enforcement of the Biba security model has the following implications:

1. A subject S can read an object O if and only if the integrity level of S is less than or equal to the integrity level of O. This ensures that a subject of a higher integrity classification cannot read data from an object of lower integrity classification
2. A subject S can write to object O if and only if the integrity level of O is less than or equal to the integrity level of S. In this case, a subject with lower integrity classification cannot write data to an object of higher integrity classification

3. A subject S1 can invoke another subject S2 if and only if the integrity level of S2 is less than or equal to S1. This keeps a low integrity subject from invoking a high integrity subject, which could then modify information on its behalf

The Biba integrity model complements the Bell-LaPadula security model in that it preserves the integrity of information in the system that implements the model and prevents data modification from unauthorized parties or from less reliable sources of lower integrity.

Both the Bell-LaPadula and Biba security models describe properties and rules that control access to classified information. Theoretically, systems which implement internal mechanisms to strictly adhere to these models protect against the leakage of high value, sensitive information. These models have shown to be consistent with rules defined in most organization's security policies for the management of classified information.

A lot of research and implementations have been conducted to develop MLS systems. However, due to the high complexity of such implementations and the high cost associated with these products, there is a limited number of MLS systems available in the commercial products.

So, despite all the effort to develop MLS systems and models, most organizations are still using separate networks and systems to process classified and sensitive information. Military services use MLS systems only for specialized operations where specific sharing of information with different classifications is required. In most military departments, classified information is still managed in separate systems and networks. To permit the use of computer systems to process and store classified information securely, systems of higher assurance are required. The following section discusses the concept of system assurance.

6. Assurance

When computer systems are implemented to enforce organizational security polices and rules, it is essential that the internal mechanisms of the computer systems are correctly implemented and that they strictly enforce these rules. How are computer systems assured that they actually provide the claimed security functionalities and that these functionalities are effective and implemented correctly? Assurance of the computer system is the confidence that the claimed measures, in this case security measures, are implemented correctly and that they enforce the rules according to some security policies. To achieve a certain level of assurance in the system, computer systems have to undergo some IT security evaluation, certification and accreditation conducted by independent evaluators or authorities. These independent evaluators and authorities will evaluate the systems based on a set of well-defined assurance criteria, which are derived from the users' organizational security objectives and security policies.

The most common security evaluation of information technology systems and products is the Common Criteria (CC) [CC 2005]. CC is an international standard for evaluating computer security. It defines a set of potential security requirements in terms of functional and assurance requirements. IT products and systems are evaluated based on these security requirements to provide assurance that the products do in fact meet the claimed security functionalities. The assurance validation of the security measures are benchmarked against seven Evaluation Assurance Levels (EALs), numbered from 1 to 7, with the higher EALs requiring more vigorous testing and formal evaluation to extensively validate the security mechanism to ensure that it is correctly developed and effective in countering the identified threats.

At the lowest assurance level, that is EAL1, functional testing is conducted to ascertain that security features of the component comply with the functional and interface specifications of the system. An EAL1 assurance component functions in a manner consistent with its documentation and it provides useful protection against identified threats. As the product is evaluated for higher assurance, more methodical testing and formal evaluation will be conducted. For higher assurance systems, that is, systems evaluated at EAL 5, 6 and 7, the designers of these systems have to provide a chain of evidence demonstrating that the design of the systems is based upon a provable formal mathematical model. For an EAL7 evaluation, the formal models are supplemented with formal functional specifications and a correspondence between the two formal representations is proved. Informal mapping is used to demonstrate a correspondence between various lower levels of system design specification and the formal representation. Eventually, evidence must be produced to show that the implementation of the different layers in systems and the interfaces between these layers map to the formal specifications. To satisfy EAL7, the complexity of the system design will also have to be minimized. EAL7 assurance is applicable to components developed for use in extremely high risk situations or where the high value of the assets they contain justifies the requirement for such evaluation. Higher assurance systems are evaluated based on EAL5, EAL6 and EAL7 criteria.

E. SUMMARY

Information can be protected without MLS. MLS makes it less costly because there is less equipment and it requires fewer people to manage. It also makes it easier to access real-time lower-level information. But it comes with more risk, and therefore there needs to be higher assurance systems. MLS systems are very useful to secure and manage highly valuable classified information. They provide a mechanism for controlled sharing of classified resources and information. As we transform into the digital era, more and more of our functions and assets will be migrated into the digital platforms. Future battles might be fought over the cyber domain; therefore, it is important that we have the necessary and reliable mechanisms to protect these digital assets.

The next chapter will present the research questions of this thesis and at the same time identify the educational goals of the CyberCIEGE scenario developed as part of this thesis.

III. SCENARIO GOALS

A. SCENARIO OVERVIEW

The purpose of this thesis is to answer the following research question: Can a scenario be developed to illustrate the principles of Multilevel Secure (MLS) systems? An ancillary question is: how can MLS systems be deployed to protect different classes of sensitive information in the military environment? This scenario should address the issues concerning simultaneous access to information with different sensitivity levels. The player will be introduced to the management of different classifications of information. He will have the ability to make security-related decisions regarding how to enforce security and policies, in order to control access to sensitive information in a military-like networked environment. This thesis focuses on the tensions and trade-offs between the use of air-gapped single level systems and the interconnection of such systems using multilevel secure components.

For the rest of this thesis, players will be referred to as officers and students who are using the CyberCIEGE system to learn IA concepts. Users will be the virtual characters that are part of the scenario in the CyberCIEGE game.

B. SCENARIO EDUCATIONAL GOALS

As explained in Chapter II, there is currently no available tool to validate IA concepts learned and acquired from lessons and textbooks, except to carry out actual implementations of such networks. The development of the scenario in this thesis is to provide a more realistic and effective alternative to the lecture-style training in IA. This scenario will use the CyberCIEGE game as the tool to introduce and train personnel in the issues highlighted in the research question posed above. The following sections will describe the intended players of this scenario, the educational goals derived from this scenario, and how elements of CyberCIEGE can be used to achieve these educational goals.

1. Intended Players

The intended players for the CyberCIEGE game are government and DOD employees, both civilian and military personnel. The U.S. government places a lot of emphasis on IA training, especially with the endorsement of the E-Government Act of 2002 [H.R. 2458]. The E-Government Act of 2002 specifically requires all government agencies to have agency programs to provide, among other training topics, security awareness training. The purpose is to educate all personnel, who support the operations and manage assets for the agency, regarding the information security risks associated with their duties, and their responsibilities in complying with agency policies and procedures designed to reduce these risks. DOD, as a frontrunner in the development and deployment of information technology, also has clearly spelled out directives to promote the training of IT personnel to raise their IA awareness [DOD 85701]. DOD Directive 8570.1 states that all DOD Information System personnel must have their initial IA awareness training before accessing DOD information systems. This training will be refreshed annually to ensure continual awareness and compliance to the IA policy. All these programs provide government employees and military officers with the basic knowledge of IA. To constantly provide IA training and to raise the awareness of information security, DOD and the Defense Information System Agency (DISA) have sponsored a web portal, “Information Assurance Support Environment - The DOD IA Portal”, to publish information about security issues and to help personnel keep abreast of the latest developments in this area.

CyberCIEGE complements these efforts by providing a platform for players to apply and validate the IA concepts acquired in the agency programs. As a computer game, CyberCIEGE allows players to implement their concepts, experiment with different configurations and evaluate the effects. In doing so, players learn and appreciate the principles behind the decisions they have made while playing the game. Through role-playing the different scenarios, players can better relate to the IA issues and the configuration of the IT equipment set up in their office environments.

As different players will have different levels of IA knowledge and training experience, the CyerCEIGE game can be designed with different scenarios to address different aspects and levels of IA training. In particular, the scenario developed for this thesis focuses on the controlled access to and management of classified information of different sensitivity levels and the use of the MLS components to secure such access. Therefore, there are two groups of officers who will personally experience similar scenarios in their tour of duties: the first group will be authorized officers who have some basic understanding of IA and have regular access to classified information, and the second group is the IT developers who implement secure networks and MLS systems. The scenario is not restricted to these two groups of people; officers who are interested in knowing more about integrating secure networks and understanding MLS systems may also benefit from executing this scenario.

a. Privileged Officers

The targeted players for this scenario are authorized officers who have access to sensitive information, that is, information classified, for example, as Confidential, Secret or Top Secret. By virtue of the sensitivity of this information, these officers will have to manage their access to such information and ensure that they comply with the security policies. The scenario for this thesis will introduce the requirements for access to information of different classifications.

Players of the scenario will have to make decisions and implement a secure infrastructure to protect these accesses. Through this scenario, players will be able to apply the concept of trusted systems and devise different strategies to apply to the game. In the process they will understand correct implementations for securing systems.

b. Developers of Secure Networks

Developers of secure networks plan and design the computer and network infrastructure. They understand the mechanisms of each of the components, their purposes, and how they can be installed in the network to provide the necessary services. Networking equipment is installed to connect computer systems to form local connections or to connect to other networks to form larger networks. Security equipment such as firewalls, filtering routers, and IDS are put in place at strategic network points to monitor and protect segments of the network. MLS systems are used to manage information of different classifications. Networks and information flowing into the MLS systems must be controlled and properly labeled with the correct security classification. All of these, and many other information security mechanisms, have to be put in place in order to enforce the overall security policy and provide assurance that the valuable information assets are as securely stored and managed in the IT setup as they are required to be as stated in the organizational security policies. Developers can execute the various scenarios to understand how these mechanisms work and how they can be deployed to secure the IT infrastructure for MLS systems. This scenario will provide the developers with a better understanding of security implementation and improve the developer's ability to make coherent design decisions to enforce information security.

c. Others

Besides the above two groups of people, other government employees and officers can also benefit from playing the CyberCIEGE game. Different CyberCIEGE scenarios will reinforce different information security concepts that are taught in the IA awareness courses. Players of the game will be refreshed with the IA concepts they have learned and they will be able to relate them to the real world applications in their offices. Lastly, CyberCIEGE raises these players' awareness of the security policies and the roles they play to enforce them.

2. Educational Goals

The purpose of this thesis is to develop a Scenario Definition File (SDF) that implements a scenario that is both educational and entertaining. The primary purpose of this SDF is to illustrate specific IA concepts concerning the management of classified information and to introduce the IT equipment and mechanisms that would provide a secure enough environment for classified information to be protected and accessed by authorized personnel. The scenario developed for this thesis is designed in a modular and sequential approach, such that the players will learn more in-depth concepts as they proceed further into the game. Issues concerning the protection and control of classified information will be gradually introduced to the players as they complete each phase and continue into the next higher level. New operational requirements will be introduced incrementally and the players are expected to fulfill all of these requirements in order to successfully complete the game. It is expected that players will fail to complete the game at their initial attempts. As players rerun the game, they will gain more experience from the mistakes they have previously committed and from the explanations provided by the in-built CyberCIEGE encyclopedia. These experiences and explanations will enlighten the players and reinforce the IA concepts for them. Having understood the essence of these concepts, players will be able to apply them in the game and eventually complete the scenario.

This scenario is designed with three educational goals, as described in the later part of this section: physical security is an integral part of information security, separate networks as an approach to manage information of different classifications, and controlled sharing of classified information. The intention is to convey these IA concepts to the players as they execute this game. Players will learn these concepts and appreciate how the computer and network infrastructure can be made secure to provide the necessary control and assurance to the IT system.

To illustrate assets of different values, this scenario defines and uses the following secrecy classifications:

TRULY SENSITIVE: The highest classification in the scenario. It is used on assets that the compromise of which will have devastating impact on all military operations and missions planned.

SENSITIVE: This classification is used on assets that the compromise of which will have grave impact on all military activities.

UNCLASSIFIED: This is the lowest classification in the Command and Control (C2) scenario. Assets of this classification have no secrecy value.

The detailed descriptions of these labels are defined in Chapter IV. All assets in the C2 scenario will be assigned to one of these classifications to create values for the assets which the player must protect.

In the design of this scenario, there are three classes of networks: a TRULY SENSITIVE network to access critical military intelligence information, a SENSITIVE network to access classified information disseminated by the Allied Forces, and the UNCLASSIFIED network where access to the Internet is provided. To focus the game on the controlled management of classified assets, the scenario has some defaults settings:

- The whole C2 center is designed as one zone and entry is only granted to users having TRULY SENSITIVE security clearances.
- All users in the scenario are already cleared up to TRULY SENSITIVE so that players do not have to conduct background checks for all the users in the command center.
- In real world implementations, DAC policies are implemented within a single level network. However this thesis will not address the enforcement of discretionary policies.

a. Physical Security Is an Integral Part of Information Security

Different levels of physical security should be implemented to protect assets of varying value. The higher the value of these assets, the stronger should the physical security be. The value of the organization’s assets and its motive to be attacked by adversaries, known as *motive to attack*, will determine the level of physical security to be put in place to protect these assets. The scenario developed for this research is used to illustrate these points.

In CyberCIEGE, assets have value to the organization. They can be information needed for daily operations, or important information like military intelligence, tactical strategies or business plans, which are critical to the organization’s success. CyberCIEGE assets also are a motivating factor for adversaries to compromise them. Adversaries will engage in attacks from all possible venues to try to gain access and capture these assets. In this scenario, TRULY SENSITIVE assets are given a very high motive value for attackers. In order to protect these assets, strong physical security must be enforced. Otherwise, the game’s attack engine will compromise the TRULY SENSITIVE asset. And by selecting very strong physical security, e.g. guards, the player will be reminded of the value of the TRULY SENSITIVE assets.

In CyberCIEGE, sites are offices and buildings where the users work. Each site is divided into one or more zones. A zone is a work area in the scenario that is controlled by a set of physical security policies. These policies are enforced by physical security measures. Players have to determine the level of physical security to be installed at each zone to control the access and monitor movement into these zones. These physical security measures protect the components and assets that are placed within the zone. In this scenario, to achieve the goal for protecting a TRULY SENSITIVE asset, players have to purchase and implement security components that collectively are strong enough to counter the adversaries' motive to attack. In doing so, the player learns about the strength of each security measure and that higher classified assets will require greater physical protection.

b. Separate Networks

Chapter II, Section D describes why organizations tend to maintain separate networks to manage information of different sensitivities, for example TRULY SENSITIVE and SENSITIVE. And it explains why connections between these separate networks are avoided unless there is a strong operational need.

This scenario will require the player to provide users with computer and network resources to work on both TRULY SENSITIVE and UNCLASSIFIED assets. This is achieved using CyberCIEGE user goals. In the first two phases of the scenario, users will have individual goals that can be achieved by separately accessing the TRULY SENSITIVE and UNCLASSIFIED assets. No one goal will require access to both.

The scenario uses CyberCIEGE conditions and triggers to guide the players to set up the necessary computer and network equipment for the separate accesses to TRULY SENSITIVE and UNCLASSIFIED assets. CyberCIEGE conditions are configured in the scenario to test if the players have provided simultaneous access to both assets via interconnecting the networks of different classifications. If such a condition exists, the scenario will trigger message events to warn the player of a security violation. Players have to remedy the network configuration. Upon failure to do so, the game engine will generate attacks to capture and disclose the TRULY SENSITIVE asset which can be accessed via the UNCLASSIFIED network. Through achieving the goals in the game, the player will learn the importance of separating networks of different classifications.

c. Controlled Sharing of Classified Information

Phases 1 and 2 have separated goals for accessing individual assets; there is no requirement for simultaneous access to multiple assets at different classifications. In Phases 3 and 4, players have to fulfill goals that require simultaneous access to multiple assets of different classifications. They will have to configure interconnections between systems and networks of different classifications while protecting the confidentiality of classified information.

Phase 3 of the scenario challenges the players with a CyberCIEGE goal to provide a TRULY SENSITIVE user with the access to both the TRULY SENSITIVE intelligence asset and SENSITIVE Allied Force asset simultaneously. The TRULY SENSITIVE asset is stored in the server room at the C2 center, while the SENSITIVE asset is stored at an offsite office which can only be accessed via a network connection. The network connection between the offsite office and C2 center is protected via link encryptors. The physical security of the offsite zone will be selected such that it is sufficient to protect SENSITIVE information, but not TRULY SENSITIVE information. Thus to fulfill the user's goal of simultaneous access, players have to set up high assurance, MLS components to secure the interconnection. The CyberCIEGE scenario offers a variety of workstations, a mixture of both low and high assurance systems. Players will be tempted to purchase the low assurance workstations as they are cheaper and the players have a limited budget. Low assurance systems provide less confidence in the correctness and completeness of security implementations and hence when deployed, these systems will be more vulnerable to attacks. Players will have to select high assurance systems for this deployment. For the configuration of an MLS component, proper labeling of connections to the MLS workstation and training for the user's interaction with the MLS workstation will be required, as these MLS components have more sophisticated procedures to enforce security policies and protect the classified assets. If the players provide insecure connections between the networks, the game engine will compromise the TRULY SENSITIVE assets by defeating the offsite physical security to gain access to the SENSITIVE network through which TRULY SENSITIVE information can be accessed.

In Phase 4 of the scenario, players will need to scale the interconnections to provide simultaneous access to the UNCLASSIFIED asset on the Internet. That is, players will have to provide access to TRULY SENSITIVE, SENSITIVE and UNCLASSIFIED assets simultaneously. Unlike phase 3 where the remote asset is classified SENSITIVE and stored in a secure offsite office, assets on the Internet are open source resources and the network is accessible by everyone, including the adversaries. Hence, assets on the Internet have lower or little security protection and the Internet network is more prone to attacks. Therefore, the risk involved in connecting to the Internet is much higher than connecting to an Allied Force asset at the secure remote office.

The scenario is designed to use conditions and triggers to stimulate cyber attacks on the IT infrastructure. This is done to control when to introduce attacks to the systems so as to allow players to better understand the impact of their decisions. However, such attacks are of fixed frequency, and both the connections to the SENSITIVE network and to the UNCLASSIFIED Internet are subjected to the same rate of attacks. This is unlike real world implementations where the assets on the Internet are more frequently attacked than assets protected in a secure office.

On the other hand, CyberCIEGE is able to overcome this shortcoming with different attack values. CyberCIEGE attack triggers have randomly generated attack values which determine the strength of these attacks. These attack values are compared to the physical security of the assets and network to determine if these assets and network are successfully attacked and compromised. Since the Internet resources have little physical security protection, the values of their physical security will be lower than those of the secure offsite office. Thus there will be more attacks that successfully compromise the resources on the Internet as compared to the attacks on the secure offsite office. When the players connect the TRULY SENSITIVE network to the Internet and to the SENSITIVE Allied Force network, the TRULY SENSITIVE network will experience more attacks from the Internet connection. Thus, it is important that proper labeling is done on the network connections to the MLS systems to ensure that appropriate security enforcements are applied to the connections of different classifications.

Phase four of the scenario demonstrates the relative risks involved in connecting classified networks to the Internet as compared to connecting it to secure remote networks. The players will understand these risks as they configure the connections between resources of different classifications.

To complete the scenario, players will have to meet all of the objectives in each phase of the game. Each of these objectives will test the players' understanding of the above concepts. Players will be exposed to the security issues mentioned above; they will have to make decisions regarding what computer and network equipment to buy and how to implement them in order to comply with and enforce the security policy. To complete and win this scenario, players will have to work within the allocated budget, and the implemented computer and network infrastructure will have to withstand attacks for over two days.

C. SUMMARY

This chapter has described the intended players and educational goals for this scenario. The next chapter will provide more details regarding the actual implementation of the scenario.

IV SCENARIO OUTLINE

The Command and Control (C2) center scenario is developed to answer the thesis research question highlighted in Chapter III. This chapter describes the details of this scenario. The scenario is intended to achieve the educational goals highlighted in Chapter III, and it follows the described strategy.

A. SCENARIO OVERVIEW

The scenario simulates a C2 center for military operations. The center is the fusion point of operational and tactical information and intelligence that will provide operational commanders with the necessary situational awareness for their deployments. Such information is essential to any mission as it provides the troop commanders with field information that is critical to the success of their missions. The command center acts as a depot for data, information and knowledge to aid in all military decisions.

1. Layout of the Scenario

The scenario consists of two locations: the C2 center and the remote offsite office. The layout of the C2 center is shown in Figure 1.

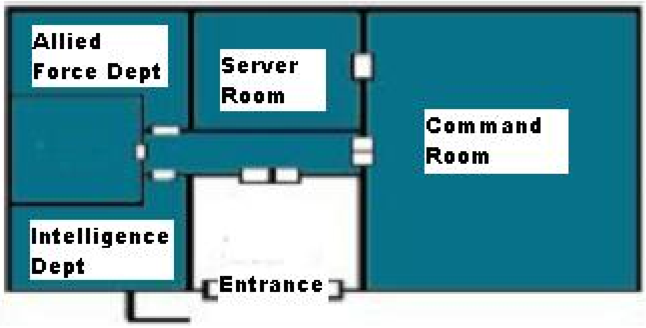

Figure 1. Layout of C2 center

A number of departments make up this C2 center. The intelligence department, which resides on the bottom left room of the C2 center, gathers information about the enemy, terrain and area of operations. The top left office is occupied by representatives from the Allied Forces. They serve as the liaison officers between their countries and the commanders in the C2 center. The server room is in the top middle of the C2 center and it houses all the server and network equipment. The main C2 operations are carried out in the command room on the right of the C2 center. Military activities like force deployment, readiness assessment and mission planning are conducted in the command room.

The offsite office is the secure office for the Allied Forces Headquarters and it consists of a single room.

2. Narrative of the Scenario

The following is the initial brief to the scenario. It provides a description of the context of the scenario, and the goals and requirements for the player.

> Welcome to the Command & Control Center. This is the nerve center of all military operations; it is here that all military planning, force deployment, readiness assessment and mission planning are conducted and decisions on these military activities are made. You have an important role in making this center work. As the head of Information Technology and Security, you have to provide the necessary infrastructure so that the command and staff officers can operate and develop the situation pictures of the various theatres of operations. These situation pictures will provide the situational awareness needed for military planning and they will serve as important sources of information for decision making.
>
> Your scope of work will involve setting up and maintaining the center's computer and networking infrastructure, so as to keep the staff productive. While doing so, you have to ensure that the classified assets in the C2 center are protected. This classified information includes military TRULY SENSITIVE intelligence information and SENSITIVE information contributed by the Allied Forces. You are given an initial budget to buy components, software, IT staff, etc. You will receive additional bonuses when you achieve certain significant milestones. You will have to identify the goals of the users, make choices about the types of components to purchase, and how to set up these components. If your choices compromise the security of the assets in the C2 center, you will be penalized monetarily. However, if your choices meet operational requirements and at the same time protect the classified assets, you will proceed to the next phase of the game. You win the game if you successfully complete all the objectives within the budget allocated.

> Click the "CLEARANCE" button for information about the values of the classified assets. The scenario is divided into several phases. You must complete all objectives of a phase to move to the next phase. Use the OBJECTIVES button in the OFFICE tab to see your objectives for each phase. Press "e" at any time to view the CyberCIEGE encyclopedia, which includes a "How To" section. Press "k" to view keyboard shortcuts and navigation keys. Click the "OFFICE" tab and click the green key "play" button to begin play. Good luck!

B. ELEMENTS OF THE SCENARIO

This section describes the elements that constitute the C2 scenario.

1. Users

Users are the simulated characters within the scenario. They interact within the virtual environment and are affected by the decisions made by the player. In the C2 center scenario, there are two groups of users: staff officers who operate in the C2 center and the support staff that provides peripheral support to the operations of the C2 center. The staff officers are Maj. Keith, Capt. George, Lt. Deborah, Lt. Robbie and Lt. Cristiano. And the members of the support staff are Matthew and Tommy. All the personnel in the C2 centers are security cleared to TRULY SENSITIVE.

Maj. Keith is the commanding officer in charge of the C2 center. He keeps abreast of the latest developments in various theaters of operations by constantly studying the changes in the situations that occur in the places of interest. He reads the reports and classified analyses submitted by his staff officer, Capt. George, and accesses the Internet for current affairs information. If there are sudden changes of events or occurrences of unexpected activities which have a drastic impact on military operations, Maj. Keith will convene higher-level meetings and update the commanders from the various military services.

Capt. George supports Maj. Keith in his duties. He processes, analyzes and assimilates military related information from various sources in order to produce timely and accurate situation reports and updates for Maj. Keith. Capt. George accesses military information mainly from two sources: the TRULY SENSITIVE intelligence information gathered from the intelligence department and SENSITIVE military operations and reports from Allied Forces. Capt. George occasionally accesses the Internet to download articles, as instructed by Maj. Keith, in preparation for high-level meetings. Therefore, Capt George has the goal to simultaneously access the Intelligence, Allied Forces information and sources from the Internet, as described below

Lt. Deborah is from the Military Intelligence branch and she works in the Intelligence office, gathering military intelligence and storing it in the departmental server. As this information is highly sensitive and valuable to military mission planning, Intelligence information is classified TRULY SENSITIVE and has to be kept in the strictest confidentiality. Lt. Deborah needs to access the Intelligence asset in order to complete her job. In addition, Lt Deborah also accesses the Internet to monitor activities and reports gathered from the Intelligence. Therefore she has two separate goals: access to Intelligence information and access to the Internet.

Lt. Robbie and **Lt. Cristiano** are from the Allied Forces. They are attached to the C2 centers as liaison officers from their respective countries. They keep in contact with the military headquarters in their respective countries and exchange military information relevant to the C2 center’s operations. Such information is important, as it provides military status of the respective countries and intelligence gathered, which is critical to coalition missions. Information from the Allied Forces is stored in a separate server at the remote Allied Forces Headquarters and is classified SENSITIVE.

Matthew is the IT support staff employed to provide computer and network support in the C2 center. As the C2 center deploys a variety of IT equipment, from workstations to servers and network equipment, Matthew will be in charge of providing the first level of support and troubleshooting to resolve any operational hiccups. Matthew has a diploma in computer science and he is capable of maintaining the equipment and ensuring that it is configured according to the organizational IT security policy. He has a skill value of 90 out of 100 for software and hardware skills, and a value of 95 for his initial training.

Tommy is a trained security guard employed to beef up the security of the C2 center. He is armed and can be deployed to perform access control at the building entrance by ensuring that all personnel display proper passes or identification before entering the C2 center. Tommy has a skill set of 90 and an initial training value of 90. He is capable and will patrol the perimeter of the center if required.

2. Mandatory Policy

The following classifications are used in the C2 center scenario. All assets and security clearances have been assigned with one of these classifications. The game engine will enforce Mandatory Access Control policy to enforce the protection of assets according to these classifications. For example, users with a SENSITIVE security clearance will not be able to access assets classified as TRULY SENSITIVE.

TRULY SENSITIVE: The highest classification in the scenario. It is used on assets that, if they are compromised, will have devastating impact on all military operations. Mission plans based on such information will be potentially foiled. The TRULY SENSITIVE classification has a secrecy value of 100,000 points and an attacker motive value of 800. Users need to have high background checks in order to access TRULY SENSITIVE assets.

SENSITIVE: This classification is used on assets that, if they are compromised, will have grave impact on all military activities. While the impact is serious, it would not determine the success or failure of any military mission. This classification has a secrecy value of 60,000 points and an attacker motive value of 400. Users are required to have medium background checks to access SENSITIVE assets.

UNCLASSIFIED: This is the lowest classification in the C2 scenario. Assets with this classification have little or no value to the organization. Thus their disclosure will not cause any damage to the military operations in the C2 center. This classification has no secrecy value and zero attacker motive value. Anybody can access UNCLASSIFIED assets.

3. Assets

Assets are the critical resources of the game. They are what the users need to have access to in order to be productive and happy with their work. The assets that players need to provide users access to, while ensuring their protection, are: the Intelligence information, Allied Forces information and information from the Internet.

Intelligence is one of the most important assets of any military organization, as it provides insight about the adversaries, their locations, activities and both military and political operations. Such insight is important for military planning and it can be decisive in a successful mission. Therefore, the Intelligence asset is very valuable to the C2 center and it will cost the department $1,000,000 if this asset is compromised. The Intelligence information is classified TRULY SENSITIVE and it has a very high motive value of 800 to attract potential attackers. The Intelligence asset is stored in the Intelligence server residing in the server room of the C2 center.

Allied Forces information regarding their military plans, troop deployment and intelligence, is relevant to the combined missions. Such information is important for joint planning and it provides an additional reliable source of intelligence for military planning. This information is classified SENSITIVE and it has a motive value of 400. The Allied Forces information is housed in the server at the secure remote Allied Forces Headquarters office, which has the physical security of 500.

Web pages on the Internet are rich sources of information and they provide media coverage of events happening around the world. Such information is important to keep abreast of the development in the theatres of operation and they contribute to the development of the operational situation pictures. As the information from the Internet is from an open source, it is UNCLASSIFIED and has no attack motive and no secrecy value.

4. Physical Components

The player begins this scenario with the Intelligence server residing in the server room of the C2 center and Allied Force server located in the secure offsite office. Two workstations are set up in the Allied Forces department to allow Lt. Robbie and Lt. Cristiano remote access to the Allied Forces assets.

Both the Intelligence and Allied Force servers and the workstations in the Intelligence department and Allied Force department in the C2 center are static components; the player cannot make changes to these components.

5. Networks

Some default networks are set up to connect the physical components in the scenario. For remote access to the Intelligence asset, an Internal Intel Local Area Network (LAN) is set up within the C2 center to connect the workstations in the Intelligence Department to the Intelligence server. A leased line is laid from the offsite Allied Forces Headquarters to the C2 center. This leased line is protected by link encryptors at both ends of communication and is indirectly connected to the Allied Forces server at the offsite office. At the C2 center, workstations in the Allied Forces department have remote access to the Allied Forces assets by riding on an Internal Allied Forces LAN which, in turn, is connected to the leased line.

Additional networks, LAN 1 and LAN 2, are available for the player to establish new network connections in order to achieve the assets goals described in the following paragraphs.

6. Goals

Goals are associated with users, and are used to specify assets they need to access. They determine whether the users are able to accomplish their tasks and be productive to the organization. If the users' goals are not met, users' productivity will drop and their happiness will decline. This will, in return, affect the organization's bottom line. Therefore, a player of the scenario has to provide the necessary components in order for the users to gain access to the required assets and fulfill their goals.

The following are the descriptions of the asset goals in the C2 center scenario:

Access Intelligence. This goal requires read access to the Intelligence asset. The Intelligence asset is compiled and assimilated by the Intelligence department and is stored in the Intelligence server at the server room of the C2 center. Since there is no local access to the Intelligence server, this goal requires the player to set up a workstation with network connections to the Intelligence Server for remote access. The player also has to beef up the physical security of the C2 center to protect this asset.

Access Web Resource. This goal requires read access to the resources on the Internet. As the Internet is on the wide area network (WAN), the player will have to purchase a routing device that can connect the local area networks within the C2 center to the WAN.

Simultaneous Access to Intelligence and Allied Forces Information. This goal requires concurrent access to these two assets of different classifications. In order to plan for combined military operations, Capt. George needs to assimilate the intelligence from the Allied Forces with that from his own force, so that joint planning and operations are done as overlapping and simultaneous activities. The player will have to provide a high assurance computer component with MLS capability to provide the necessary protection for the classified information.

Simultaneous Access to Intelligence, Allied Forces Information and Sources from the Internet. As the commanding officer of the C2 center, Maj. Keith keeps abreast of the latest developments in the various theaters of operation. He reads reports and classified analyses submitted by Capt. George, and accesses the Internet for current affairs information. This goal requires that the player help Maj. Keith set up concurrent access to the open source information from the Internet, SENSITIVE Allied Forces assets on the remote server and TRULY SENSITIVE Intelligence information from the server room in the C2 center.

7. Zones in the C2 center

The entire scenario is divided into two zones, the C2 center zone and the Offsite Office zone. The C2 center zone comprises the entire physical Command and Control center, including the server room, command room, the Intelligence department and the Allied Forces department. This zone is built with re-enforced walls and has key locks as the default physical security. Only the staff officers and support staff of the C2 center are allowed into the C2 center zone and they have to display their identification. These security measures constitute a physical protection value of 316 points. The player is expected to increase the physical security of the C2 center zone to protect the classified assets kept within these premises.

The Offsite Office Zone is the secure remote office housing the Allied Forces Headquarters. It has a physical security value of 500 to protect the SENSITIVE Allied Forces asset stored in the building. The player is not allowed to make changes to the components in the offsite office.

8. Conditions and Triggers

CyberCIEGE conditions are set in the scenario to check for the occurrences of certain events or situations. When these conditions occur, the CyberCIEGE game engine will execute the corresponding triggers associated with these conditions.

In the C2 scenario, the following conditions and triggers are defined.

C2 center Has 800. This condition checks if the C2 center has physical protection of at least 800 points. It checks if the player has completed the requirement for beefing up the physical security of the C2 center. If this condition is satisfied, compounded with the set up of access to Intelligence Information, the CyberCIEGE game engine will proceed to Phase 2 of the scenario.

Everyone's Assets Goals : This condition checks if all user's existing assets goals are satisfied. If they are, this condition will trigger the transition to the next phase of the scenario.

Min Cash 0**.** Player has a budget to purchase components for meeting assets goals. If he depletes the budget due to overspending or because of monetary penalties, he loses the game. This condition checks for budget depletion equal to or below zero and triggers the "No Cash -Lose" event for game termination.

Lt. Deborah has no Intelligence access. This condition checks if user Lt. Deborah has access to the Intelligence assets. This is the asset goal and part of the objective in Phase 1 of the scenario.

Capt. George has Internet access. This condition checks if user Capt. George has access to assets on the Internet. This is the goal and objective for Phase 2 of the scenario.

Capt. George has Allied Forces and Intelligence assets. This condition checks if user Capt. George has simultaneous access to the Allied Forces assets and Intelligence assets. This is one of the goals for Phase 3 of the scenario. If this condition is met, the scenario will proceed to the next phase.

Capt. George's Training is less than 60 points. This condition checks if Capt. George has sufficient user interface training to use the MLS system. If this condition and Capt. George's Allied Forces and Intelligence assets conditions are met, the scenario will proceed to Phase 4.

Capt. George has Internet Allied Forces And Intelligence assets. This condition checks if Capt. George has concurrent access to the assets from the Internet, Allied Force and the Intelligence departments. It is the goal of Phase 4 of the scenario. If this condition is satisfied, the player enters the final phase, consisting of a simple quiz.

Intelligence Server Attack. This condition checks what happens if the Intelligence assets are attacked by outsiders via the Internet connection. If it has not been attacked, this condition will trigger the CyberCIEGE game engine to simulate such attacks with motive values from 400 to 900 points.

Allied Forces Server Attack. This condition checks what happens if the Allied Forces assets are attacked by outsiders via the Internet connection. If it has not been attacked, this condition will trigger the CyberCIEGE game engine to simulate such attacks with motive values from 200 to 500 points.

Intelligence Information to Web Internet. This is a network filtering condition which checks if there is a network connection between the TRULY SENSITIVE Intelligence assets and UNCLASSIFIED web resources on the Internet. If there is, this constitutes a security violation and the CyberCIEGE game engine will simulate Intelligence Server Attacks as described above.

Allied Forces Information to Web Internet. This is a network filtering condition which checks if there is a network connection between the SENSITIVE Allied Force assets and UNCLASSIFIED web resources on the Internet. If there is, this constitutes a security violation and the CyberCIEGE game engine will simulate Allied Forces Server Attacks as described above.

All goals met. When all the goals in the scenario are met, this is the winning condition. This condition will trigger the Win state, which completes the game.

9. Phases

This scenario is divided into four phases. Each phase challenges the players in a specific area of Information Assurance. The scenario will depict some goals which the players have to fulfill. To satisfy these goals, the player will have to demonstrate knowledge of the specific IA issues being tested.

Phase 1 introduces the concept of physical security. The player has to set up remote access to the TRULY SENSITIVE intelligence information. In doing so, he has to provide adequate physical security measures in the C2 center to protect this classified asset.

Phase 2 introduces the need for Internet access. The key to completing this phase is to ensure that the connection to the Internet is separated from the access to classified information.

Phase 3 challenges the players with the need to provide simultaneous access to classified information of different secrecy levels. Players are required to establish components to provide the user with access to the TRULY SENSITIVE intelligence information and SENSITIVE information from the Allied Forces, which is located in a secure remote office.

Phase 4, the final phase, scales the requirement for simultaneous access to include the access to unclassified assets on the Internet. As the Internet is an open network, players need to understand the greater risk of connecting to the Internet and that only high assurance MLS components can enforce the necessary protection.

10. Catalog of Components

Based on the goals of the users and the objectives at each phase of the scenario, the player has to purchase new components to set up network connections to the assets. The scenario provides a list of components which the player can purchase. Some of the components relevant to this scenario are:

- Entry-Level Desktop Computers. These are low-cost general purpose desktops that can be deployed to access and process assets. They come with a full suite of office-processing software like Word Triangle for word processing, Spread Triangle for spread sheet applications and the URL2U web browser, etc. However, such computers are not certified to provide any assurance of the correctness of their implementations and they do not have in-built security mechanisms to control access to different classes of information. Examples of these computers are Blatto Desktop Select, Targo Worksaver and Lunitos AFOS systems.
- Workstations with Trusted Operating Systems. Trusted operating systems provide security mechanisms and services that protect and separate classified information. They are used for management of information with different classifications. In this scenario, two types of such workstations are available: Trusted Targo Worksaver and Green Net Client system.
- High Assurance Systems with Trusted Operating Systems. These are highly trustworthy systems with multilevel security capabilities. The only high assurance MLS system available for purchase is the Greenshade Client workstation.
- Servers are generally used to store assets for sharing or to host application programs. A variety of different types of servers are available; they range from full featured servers (e.g., Targo Server, Blato Server, Twist Off Server) to high assurance, secure servers (e.g., Green Shade Server). Specialized application servers, like email (Mail Appliance, Populos Letter Pusher) and web servers (Web Appliance, Populos Internet Slave) are also available for deployment.
- Networking routers and hubs. Routers and hubs are internetworking devices that interconnect multiple networks. Hubs are simple bridging devices that connect multiple computers or multiple networks of similar protocols. Both Wire Stuff and “Box with Wires” are reliable hubs offered by the CyberCIEGE game engine. Routers, on the other hand, are more advanced bridging gateway devices as they are able to interpret different network protocols. Therefore, routers are used to connect networks of different protocols, for example, connections between LANs and Wide Area Networks (WANs). Bit Flipper is the only high performance router offered.

Players make decisions on the choice of components to purchase and set up in the scenario that will assist the users to achieve their goals.

C. SUMMARY

This chapter provided a description of the C2 Scenario and its key elements. The player has to understand the needs of the users and provide the necessary components for them to achieve their goals. Each phase of the scenario will consist of one or two goals and when they are met, the scenario will proceed to the next phase. The player wins the game when he has completed all phases of the scenario.

The next chapter will discuss the proposed solution to the scenario and the testing done to verify that the game engine responds in an expected manner, given certain conditions in the scenario definition file.

THIS PAGE INTENTIONALLY LEFT BLANK

V. SCENARIO TESTING

This chapter describes the testing procedures conducted for this thesis. It begins by discussing the testing objective and testing methodology used for the verification of this scenario. Following that, detailed descriptions of the test cases, expected results, and actual test results are presented

A. PURPOSE OF TESTING

The scenario developed for this thesis teaches the players the educational goals, as described in Chapter II. The scenario provides feedback to the players to guide them through the scenario. Players make decisions while going through the scenario. If the decisions are correct, the scenario will respond with positive feedback to encourage the players to proceed. If the players make some incorrect decisions, the scenario will provide immediate negative feedback so that the players are aware of their mistakes. Players learn by observing the feedback generated by the scenario.

The purpose of this testing is to demonstrate that the feedback in the scenario is consistent with the real-world expectations. Test Cases were defined to verify the scenario. Each test case describes a situation in the scenario that teaches the player one of the designated educational goals. The expected results based on real-world expectations were also defined. The scenario was then executed according to the test cases and its behavior was observed. If the observed results matched the expected results, the scenario was verified to be correct. If they did not match, the scenario was not behaving according to the real-world expectations and thus needs to be corrected.

In each test case, two types of tests are considered. First, the scenario is tested with the anticipated correct solution of the game. This is to verify that the game executes according to the design of the scenario. The solution to the game describes the steps necessary to achieve the goal of the scenario. In other words, if the players make choices as stated in the solution, the game should provide positive feedback and progress through the phases, leading the player to completing the game. Second, the scenario was tested against expected alternatives or failure conditions. When the players makes bad security choices and hence configures the components differently, the game should respond with negative feedback. Note that there might be more than one solution to the game but the solution tested is based on the design intended to educate players on specific IA concepts.

B. TEST CASES

Three sets of test cases were defined, each corresponding to one educational goal, as described in Chapter II. The test cases are organized into three subsections. The first subsection defines the scope of the test, which is the educational goal it aims to demonstrate. It includes the test procedures to achieve these goals. The second subsection defines the expected results. It includes the expected results that should occur when the player applied the test procedures accordingly and the expected results if the player deviates from the solution. The final subsection records the actual results captured from the execution of the game. Each of the tests was executed using the same version of the game engine. This was done to prevent any anomalies that may result from different versions of the game engine. The actual results produced by each of the tests are observed and double-checked with the log files produced by the game engine to ensure that the observation corresponds with the behavior of the game engine. The actual results were compared to the expected results to verify that the game responds as expected.

1. Test Case 1: Physical Security

a. Scope of Test Case

Test Case 1 focuses on the need for physical security which is the first educational goal as stated in Chapter II. In the scenario, user Lt. Deborah has the Access Intelligence goal, as described in Chapter III. Therefore, the player has to set up a computer terminal in the Intelligence office with a network connection to the Intelligence server, thus extending the access of these assets beyond the server room. As the TRULY SENSITIVE Intelligence assets have an attack motive value of 800, the player will have to increase the physical security of the C2 center which has a default physical protection value of 316. Therefore, the player is expected to:

i) Purchase a computer workstation, place it at the Intelligence Department office and connect it to Internal Intel LAN.

ii) On the zone tab, select the C2 center and purchase the following physical security settings for the C2 center Zone.

- Guard at door
- Prohibit media
- Prohibit phone services
- Good Zone Alarm
- Surveillance cameras
- Badges required
- Cyber lock

b. Expected Results

If the player follows the steps to the solution as highlighted in the above paragraph, the scenario will complete Phase 1 of the game and proceed to Phase 2.

If the player does nothing to improve the physical security, or does not have enough security measures, the CyberCIEGE game engine will generate outsider break-in attacks to compromise the assets.

If the player does not provide a workstation or network connection to fulfill Lt Deborah’s Access Intelligence goal, Lt Deborah’s productivity will drop and this will reduce the efficiency of the C2 center, and the player will incur monetary penalties.

Table 1 summarizes the tests in Test Case 1.

Test ID	Description	Expected Results
Test Case 1a	The player provides a workstation for remote access to Intelligence information. The player also increases physical security of the C2 center beyond 800 points	Lt. Deborah will achieve her objective to access the intelligence information.
Test Case 1b	The player provides a workstation for remote access to Intelligence information. The player also increases physical security but keeps it below 800 points.	Lt. Deborah will have access to the intelligence information, but the assets will be stolen by external attacks
Test Case 1c	The player provides a workstation for remote access to Intelligence information. But the player does nothing to improve the physical security.	Lt Deborah will have access to the intelligence information, but the assets will be stolen by external attacks.
Test Case 1d	The player does not provide a remote workstation or the connection of the workstation to the Intelligence server	Lt Deborah will complain and the available budget for the scenario will be reduced.

Table 1. Test Case 1 Expected Results

c. *Actual Results*

The following table (Table 2) captures the actual results and identifies where the game meets the expected results.

Test ID	Actual Results	Meets Expected Results
Test Case 1a	Lt. Deborah achieved her goal	Yes
Test Case 1b	Lt Deborah had access to Intelligence information, but this information was later stolen. As a result, the player incurred monetary penalties	Yes
Test Case 1c	Lt Deborah had access to Intelligence information, but this information was later stolen. As a result, the player incurred monetary penalties	Yes
Test Case 1d	Intelligence information was stolen and the player incurred monetary penalties	Yes

Table 2. Test Case 1 Actual Results

As shown in Table 2, the actual test results meet the expected results. When the assets are extended to a control room of lower security, and left unprotected, they will quickly be compromised, either by unauthorized disclosure or because the workstation containing the assets will be stolen. Increasing the physical security will increase the protection of the assets, however sufficient security measures must be installed to thwart physical attacks on the assets.

2. Test Case 2: Separate Networks

a. Scope of Test Case

Test Case 2 focuses on the need for separate networks. It emphasizes the need to provide different levels of security protection for information of different classifications, and the need to manage them separately. This test case stretches across the first two phases of the scenario. In Phase 1, user Lt. Deborah has a goal to access the TRULY SENSITIVE Intelligence assets which has an attack motive of 800. In Phase 2, Lt. Deborah has another goal to access UNCLASSIFIED web pages on the Internet, which have a zero attack motive.

The solution to this test case is to set up two separate computer systems; one attaches to the TRULY SENSITIVE Intelligence network and the other attaches to the Internet. This will allow Lt. Deborah to have access to both assets. There should not be any interconnection between the two networks or connection between these two computer systems. Therefore, the player is expected to:

i) Purchase a computer workstation, place it at the Intelligence room and connect it to Internal Intel LAN.

ii) Purchase a second computer workstation and place it at the Intelligence room.

iii) Purchase a router and place it in the server room. Establish an Internet connection using this router.

iv) Connect the second computer to this router.

b. Expected Results

Step i) is part of Test Case 1, thus it would have been tested. When the player proceeds with steps ii) – iv), he will have completed Phase 2 of the scenario. The game will proceed with Phase 3 of the scenario.

However, if the player uses the computer terminal set up in Phase 1 and connects it to the Internet, or he selects an entry level desktop computer, or low assurance workstations with a trusted operating system, and connects it to both networks, he would have set up an insecure link between the TRULY SENSITIVE and UNCLASSIFIED networks. This workstation would not have the necessary security mechanisms to separate and enforce the access policies for this information based on their classifications. As a result, the game engine will compromise the TRULY SENSITIVE assets by defeating this low assurance workstation through the Internet connection, and thus gain access to the TRULY SENSITIVE network.

Table 3 summarizes the tests in Test Case 2.

Test ID	**Description**	**Expected Results**
Test Case 2a	The player provides two computer terminals for Lt. Deborah to access the Intelligence assets and the Internet separately. There is no interconnection between these two terminals.	Lt. Deborah will achieve her two goals to access the Intelligence information and the Internet in Phases 1 and 2 respectively. The game will proceed with Phase 3.
Test Case 2b	The player uses the computer set up in Phase 1 and connects it to the Internet	The TRULY SENSITIVE Intelligence assets will be attacked and stolen by outsider attacks coming in via the Internet. As a result, the player will lose all his money and lose the game.
Test Case 2c	The player provides a normal, low assurance workstation to connect to both the TRULY SENSITIVE Intelligence network and to the UNCLASSIFIED Internet.	The TRULY SENSITIVE Intelligence assets will be attacked and stolen by outsider attacks, causing the player to lose all his money and thus the game.

Table 3. Test Case 2 Expected Results

c. Actual Results

Table 4 captures the actual results and identifies where the game meets the expected results.

Test ID	**Actual Results**	**Meets Expected Results**
Test Case 2a	Lt Deborah achieved her two goals and the scenario proceeded to Phase 3.	Yes
Test Case 2b	Intelligence information was stolen by external attacks. The player incurred monetary penalties.	Yes
Test Case 2c	Intelligence information was stolen by external attacks. The player incurred monetary penalties.	Yes

Table 4. Test Case 2 Actual Results

Table 4 shows that the actual test results meet the expected results. The player has to provide separate computer components to provide separate access to assets of different classifications.

3. Test Case 3: Controlled Sharing of Classified Information

a. Scope of Test Case

The goal of Test Case 3 is to illustrate to the player how to set up the proper mechanisms to provide simultaneous access to information of different classifications. This test spans Phases 3 and 4 of the scenario. User Capt. George wants to achieve the goal for Simultaneous Access to Intelligence and Allied Force Information in Phase 3 and to achieve the other goal for Simultaneous Access to Intelligence, Allied Force Information and web pages from the Internet in Phase 4. The descriptions of these goals are provided in Chapter IV, Section B, Para 6.

Therefore the player is expected to:

i) Purchase a high assurance MLS workstation and connect it to the three networks.

ii) At the network interfaces to the MLS workstation, label each of the connections with the security classification of the network.

iii) Provide additional training to Capt. George such that his skill will be increased above 60 points of training.

b. Expected Results

If the player completes the three steps according to the solution, he would have completed Phases 3 and 4 of the scenario. The scenario will proceed to Phase 5, which consists of a mini quiz.

The player may decide to use an entry level desktop computer or a low assurance workstation to set up the connections to the TRULY SENSITIVE and SENSITIVE networks to meet the goal in Phase 3. However, such a configuration will provide an insecure link between the two networks, resulting in the compromise of the TRULY SENSITIVE assets as explained in Chapter II, Section B under the "Controlled Sharing of Classified Information."

The player may not provide Capt. George with the necessary training. In this case, Capt George's productivity and efficiency will suffer, and thus the player will be monetarily penalized. If the player does not label the network interfaces to the MLS system with the correct classifications, there will be no sharing of classified information and Capt. George would not be able to achieve his goals. However, if the player labels the network interfaces to the MLS system with the incorrect classifications, information with higher classification can flow to less classified networks, and the highly classified information can potentially be leaked. This is definitely a security violation.

Table 5 summarizes the tests for Test Case 3.

Test ID	Description	Expected Results
Test Case 3a	The player purchased a high assurance MLS workstation and connected it to the TRULY SENSITIVE Intelligence network, SENSITIVE Allied Forces network and to the UNCLASSIFIED Internet. He labeled all these network connections at the MLS interfaces and provided additional training to Capt. George to use the more complex procedures in the MLS system.	Player completed Phases 3 and 4 of the scenario.
Test Case 3b	In Phase 3, the player purchased a low assurance workstation and connected it to both the TRULY SENSITIVE Intelligence network and SENSITIVE Allied Forces networks.	Capt. George would have simultaneous access to the Intelligence information and Allied Forces information. However, the TRULY SENSITIVE Intelligence assets would be compromised subsequently and the player would be heavily penalized in his budget and thus would lose the game.
Test Case 3c	In Phase 3, the player did not provide Capt George with the necessary training to increase his skill sets to operate the MLS workstation.	Capt George will not achieve his goal in Phase 3 and the player will be penalized monetarily.
Test Case 3d	In Phase 3, the player did not label the network interface to the MLS system	Capt George will not achieve his goal in Phase 3 and the player will be penalized monetarily.
Test Case 3e	In Phase 3, the player labeled both the TRULY SENSITIVE and SENSITIVE network interface to the high assurance MLS system as UNCLASSIFIED	Outsider attacks will steal the TRULY SENSITIVE information by defeating the offsite physical security to gain access to the SENSITIVE network through which TRULY SENSITIVE information can be assessed.

Test ID	Description	Expected Results
Test Case 3f	In Phase 3, the player labeled the TRULY SENSITIVE network interface to MLS as SENSITIVE and the SENSITIVE network interface to MLS as TRULY SENSITIVE.	The TRULY SENSITIVE information will be exchanged and stored on the Allied Forces server. Outsider break in attacks will steal the TRULY SENSITIVE information by defeating the offsite physical security to gain access to the SENSITIVE network and thus the TRULY SENSITIVE information.

Table 5. Test Case 3 Expected Results

c. Actual Results

Table 6 captures the actual results and identifies where the game meets the expected results.

Test ID	Actual Results	Meets Expected Results
Test Case 3a	The player completed Phases 3 and 4 of the scenario.	Yes
Test Case 3b	Intelligence information was stolen and the player lost the game.	Yes
Test Case 3c	Capt. George did not achieve his goal in phase 3, and the player incurred monetary penalties.	Yes
Test Case 3d	Capt. George did not achieve his goal in phase 3, and the player incurred monetary penalties.	Yes
Test Case 3e	Intelligence information was stolen and the player lost the game.	Yes
Test Case 3f	Intelligence information was stolen and the player lost the game.	Yes

Table 6. Test Case 3 Actual Results

Table 6 shows that the actual test results meet the expected results. The player has to select a high assurance MLS system in order to securely share the classified information. The network connections to the MLS system have to be properly labeled with the security classifications of the assets in the network. Additional training is required to teach the user about how to use the more complex MLS system.

C. SUMMARY

The test cases developed for this thesis are designed to verify that the scenario achieves the designated educational goals. This testing also validated that the CyberCIEGE game engine provides feedback commensurate with real-world implementations. The testing was successfully conducted and the actual results match the expected results.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSION

A. CONCLUSION

This thesis addresses the issues concerning the sharing of classified information and demonstrates the use of high assurance MLS systems to provide simultaneous access to information at different sensitivity levels. It answered the following research question: Can a scenario be developed to illustrate the principles underlying the use of Multilevel Secure systems and how can MLS systems be deployed to protect different classes of sensitive information in a military environment? This thesis clearly shows that it is possible and how it is accomplished. Each phase of the scenario teaches IA concepts related to the management of classified information. The scenario is developed with a military background and illustrates the need for the management of classified information in the C2 center. Players are introduced to high assurance MLS workstations and they learn to configure the MLS systems to provide controlled simultaneous access to information at different sensitivity levels.

This thesis contributes a drop to the pool of IA training. It utilizes the capability of the CyberCIEGE game engine to illustrate the concepts of MLS systems and their uses in the management of classified information. Lessons learned from the development of this scenario can be used for future development of other scenarios. With the recent increased emphasis on information security and the need for IA training, the value of computer-based training will increase and gaming will become an integral part of the training tools. CyberCIEGE will continue to incorporate more pedagogically valuable scenarios and contribute to the security awareness training in the DOD.

B. FUTURE WORK RELATED TO THIS THESIS

There is some related work which can be explored for future development. This work is related to the management of classified information and can build upon the C2 scenario developed for this thesis.

1. One-way Guard Component

A MLS guard component provides a secure interface across a security boundary between systems operating at different security classifications. The guard component controls information flow across the network interface in both directions or may be restrictive to allow only a one way transfer. Such exchanges of information across a security boundary may be done automatically or may require manual review and approval done on an attached terminal. In real-world implementations, MLS guards are used to provide real-time controlled exchanges of data across networks of different classifications. They replace the airgap separation method which does not support instantaneous exchange of information. If MLS guards are modeled as one of the CyberCIEGE components, new CyberCIEGE scenarios can be developed to illustrate the controlled flow of information across networks of different security classifications, especially in the case of information flow from a network with higher security classification to a network of lower security classification and not vice versa.

2. Multiple Off-Office Sites

In the scenario developed for this thesis, both the Allied Forces HQ and web resources from the Internet reside on the same remote site, which is not realistic in a real-world implementation. This is a limitation in the existing version of the CyberCIEGE game engine which does not support multiple remote sites. An enhancement could be made to the CyberCIEGE game engine. And this would greatly enhance the realism of the scenario.

3. Specific User Training

In the current version of the CyberCIEGE game engine, a player buys additional training for the user to upgrade his IA skills and knowledge. This training is generic and covers all aspects of training; from the use of specific components, such as MLS components, to firewalls, and IA awareness training. When the player buys this additional training, the user’s training value is increased. There is no differentiation among these types of training and thus it is not intuitive to the players that training is needed for a specific operation or for the use of some components. In addition, if a particular user needs to be trained for two different components, such training cannot be simulated in the current version of CyberCIEGE. One possibility is to provide a catalog of different types of training, where each training element is specific to some IA awareness lessons or skills in the use of certain components.

4. Testing with Students

The scenario developed for this thesis was tested using test cases to verify that it provides the necessary feedback to the player and in doing so, teaches the player about the educational goals. It would also be beneficial to have the intended educational audience involved in the testing by playing the CyberCIEGE scenario. These intended players can be NPS students taking the IA courses, who could then provide valuable comments on the usefulness of the feedback mechanisms employed by the scenario, and whether they learn the intended IA concepts.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

[ANDERSON 1972] James P. Anderson, *Computer Security Technology Planning Study*, James P. Anderson & Co, 1972. Part of 2005/Spring/CS4600 Course Notes.

[Balci, 1998] Osman Balci, *Verification, Validation, and Accreditation*. Proceedings of the 1998 Winter Simulation Conference. Downloaded from the Internet on November 13, 2005: http://www.informs-sim.org/wsc98papers/006.PDF.

[BRINKLEY 2005] Donald L. Brinkley & Roger R. Schell, Applied Computer Security Associates, *Essay 2: Concepts and Terminology for Computer Security*. Downloaded from the Internet on October 17, 2005: http://www.acsac.org/secshelf/book001/02.pdf.

[CC 2005] Common Criteria, Common Criteria for Information Technology Security Evaluation, Part 1: Introduction an General Model, Version 2.3, August 2005. Downloaded from the Internet on October 31, 2005: http://www.commoncriteriaportal.org/public/files/ccpart1v2.3.pdf.

[Cohen 1990] Frederick B. Cohen, *Computer Security Encyclopedia* - Computer Viruses. Downloaded from the Internet on October 27, 2005: http://www.all.net/books/integ/encyclopedia.html.

[DOD 5200.28] Department of Defense, *Department of Defense Standard Trusted Computing Evaluation Criteria*, December 1985. Downloaded from the Internet on October 10, 2005: http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html.

[DOD 8570.1] Department of Defense, *Directive 8570.1 Information Assurance Training, Certification and Workforce*, August 15, 2004. Downloaded from the Internet on December 17, 2005 from www.dtic.mil/whs/directives/corres/html2/d85701.htm.

[FBI 2005] Federal Bureau of Investigation (FBI), *Security Clearance Process for State and Local Law Enforcement*. Downloaded from the Internet on October 31, 2005: http://www.fbi.gov/clearance/securityclearance.htm.

[FONG 2004] Gwenda Fong. *Adapting COTS Games for Military Simulation*, Defence Science & Technology Agency, 2004. Proceedings of the 2004 ACM SIGGRAPH International Conference on Virtual Reality Continuum and its Applications in Industry.

[FULP 2005] JD. Fulp, Teaching in CS3690, Network Security, Naval Postgraduate School, Monterey, California.

[GLOBALSECURITY 2005] GlobalSecurity.Org, *Operation Enduring Freedom – Afghanistan.* Downloaded from the Internet on October 10, 2005: http://www.globalsecurity.org/military/ops/enduring-freedom.htm.

[IRVINE 2003] Cynthia E. Irvine and Michael Thompson, *Teaching Objectives of a Simulation Game for Computer Security*. Downloaded from NPS intranet on October 2, 2005: http://www.cisr.nps.navy.mil/downloads/03paper_cciege.pdf.

[LAPADULA 1996] Lenonard K. LaPadula and D. Elliott Bell, *Secure Computer Systems: Mathematical Foundations and Models.* A Electronic Reconstruction by Len LaPadula. MITRE Technical Report 2547, Volume II, 1973. Downloaded from the Internet on October 10, 2005: http://www.albany.edu/acc/courses/ia/classics/belllapadula2.pdf.

[PRENSKY 2003] Marc Prensky. *Digital Game-Based Learning*, Game2train, New York, Computers in Entertainment (CIE) Volume 1, Issue 1 (October 2003), p. 21.

[SMITH 2005] Rick Smith, University of St. Thomas, Minnesota, 2005 Introduction to Multilevel Security. Downloaded from the Internet on May 10, 2005: http://www.cs.stthomas.edu/faculty/resmith/r/mls.

[ZYDA 2003] Michael Syda, Alex Mayberry, Casey Wardynski, Russell Shiling and Margaret Davis, The MOVES Institute, *The MOVES Institute's America's Army Operation Game*. Proceedings of the 2003 symposium on Interactive 3D Graphics.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Ft. Belvoir, Virginia

2. Dudley Knox Library
Naval Postgraduate School
Monterey, California

3. Ken Allen
Rivermind, Inc.
Mountain View, California

4. Hugo A. Badillo
NSA
Fort Meade, Maryland

5. George Bieber
OSD
Washington, DC

6. RADM Joseph Burns
Fort George Meade, Maryland

7. John Campbell
National Security Agency
Fort Meade, Maryland

8. Deborah Cooper
DC Associates, LLC
Roslyn, Virginia

9. CDR Daniel L. Currie
PMW 161
San Diego, California

10. Louise Davidson
National Geospatial Agency
Bethesda, Maryland

11. Vincent J. DiMaria
National Security Agency
Fort Meade, Maryland

12. Scott Gallardo
Rivermind, Inc.
Mountain View, California

13. Jennifer Guild
SPAWAR
Charleston, South Carolina

14. Richard Hale
DISA
Falls Church, Virginia

15. LCDR Scott D. Heller
SPAWAR
San Diego, California

16. Wiley Jones
OSD
Washington, DC

17. Russell Jones
N641
Arlington, Virginia

18. Steve LaFountain
NSA
Fort Meade, Maryland

19. Dr. Greg Larson
IDA
Alexandria, Virginia

20. Gilman Louie
In-Q-Tel
Menlo Park, California

21. Ernest Lucier
Federal Aviation Administration
Washington, DC

22. CAPT Deborah McGhee
Headquarters U.S. Navy
Arlington, Virginia

23. Dr. Vic Maconachy
NSA
Fort Meade, Maryland

24. Doug Maughan
Department of Homeland Security
Washington, DC

25. Dr. John Monastra
Aerospace Corporation
Chantilly, Virginia

26. John Mildner
SPAWAR
Charleston, South Carolina

27. Jim Roberts
Central Intelligence Agency
Reston, Virginia

28. Keith Schwalm
Good Harbor Consulting, LLC
Washington, DC

29. Dr. Ralph Wachter
ONR
Arlington, Virginia

30. David Wennergren
DoN CIO
Arlington, Virginia

31. David Wirth
N641
Arlington, Virginia

32. Daniel Wolf
NSA
Fort Meade, Maryland

33. Jim Yerovi
NRO
Chantilly, Virginia

34. Dr. Cynthia E. Irvine
Naval Postgraduate School
Monterey, California

35. Paul C. Clark
Naval Postgraduate School
Monterey, California

36. Michael Thompson
Naval Postgraduate School
Monterey, California

37. Michael Thompson
Naval Postgraduate School
Monterey, California

38. Prof. Yeo Tat Soon
Directory Of Temasek Defence System Institute
National University of Singapore
Singapore

39. Tan Lai Poh
National University of Singapore
Singapore

45. Ng Chee Mun
FMS students: Civilian, Naval Postgraduate School
Monterey, California